

# A Process Cycle View on Utilizing Security and Privacy Research to Realize Novel Forms of Industrial Applications and Collaboration

*Collaboration is not Evil:*

Our journey in security research for industrial use

Jan Pennekamp, Martin Henze

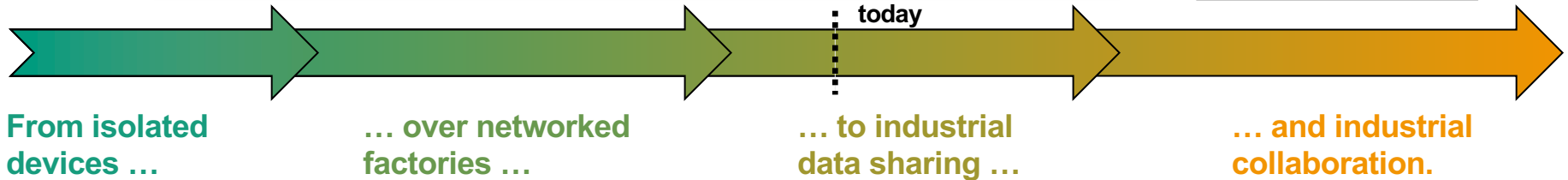
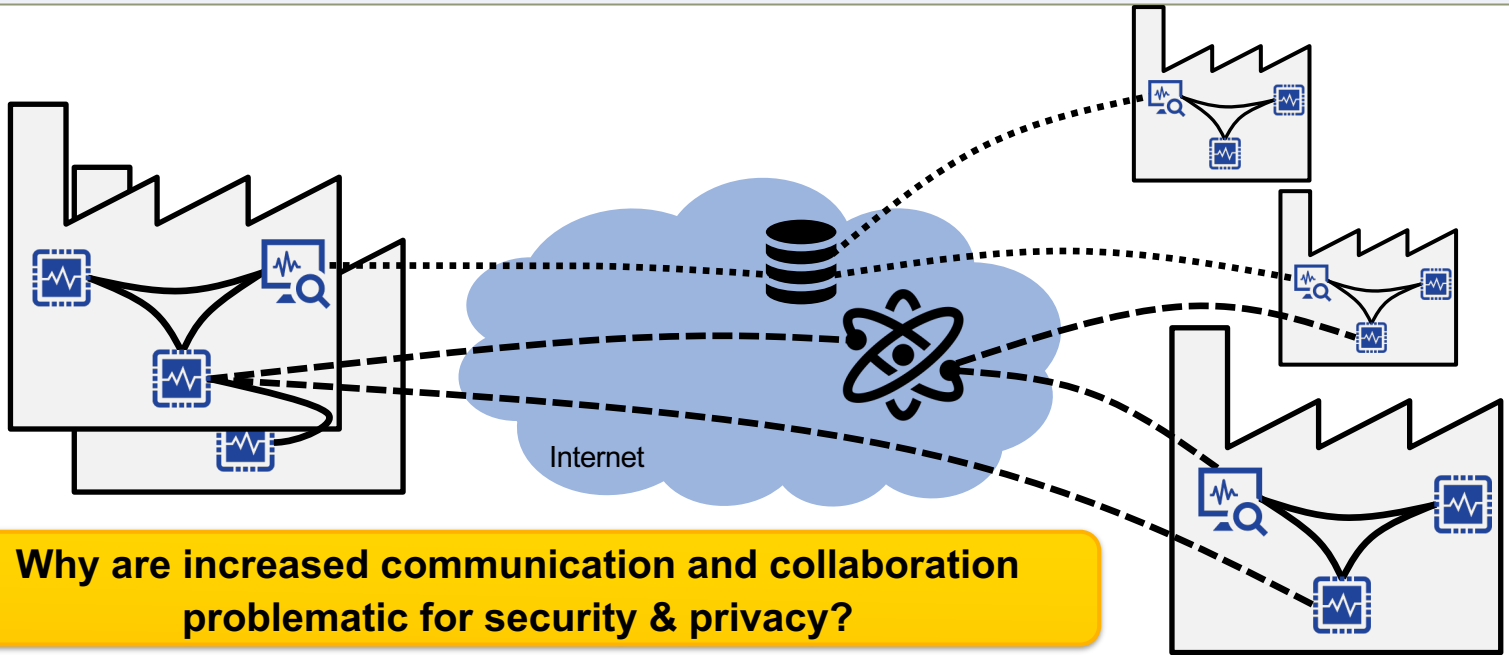
pennekamp@comsys.rwth-aachen.de

martin.henze@fkie.fraunhofer.de

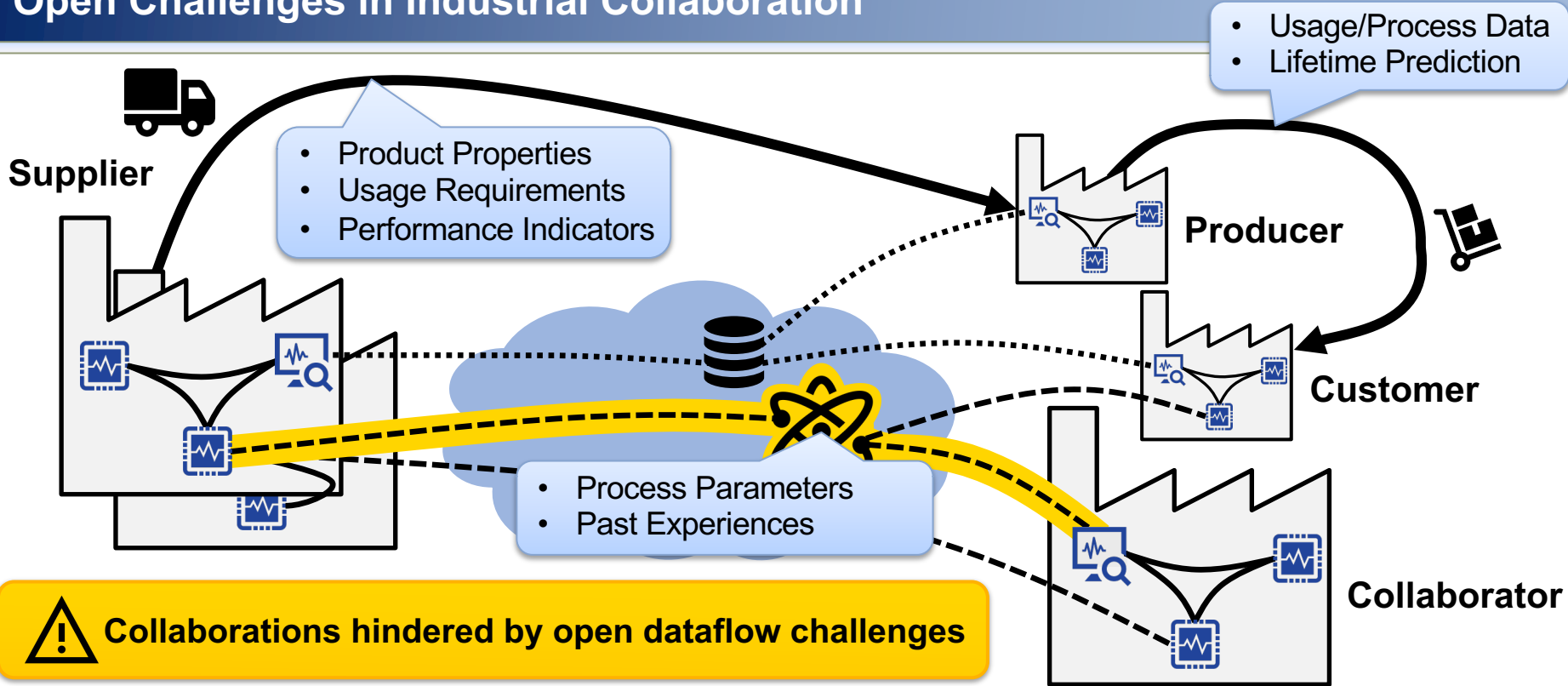
<https://www.comsys.rwth-aachen.de/>

“Austin” / LASER Workshop, 8<sup>th</sup> December 2020


# Moving from *Industrial Communication* to *Collaboration*



# Open Challenges in Industrial Collaboration

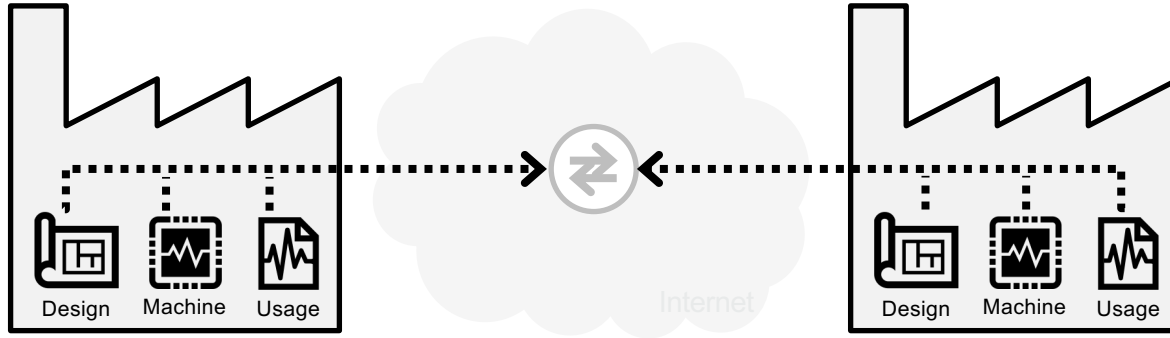


**⚠ Collaborations hindered by open dataflow challenges**

 Legacy and insecure devices and networks

 Increased exposure of devices and networks

 Loss of control over the handling of sensitive data

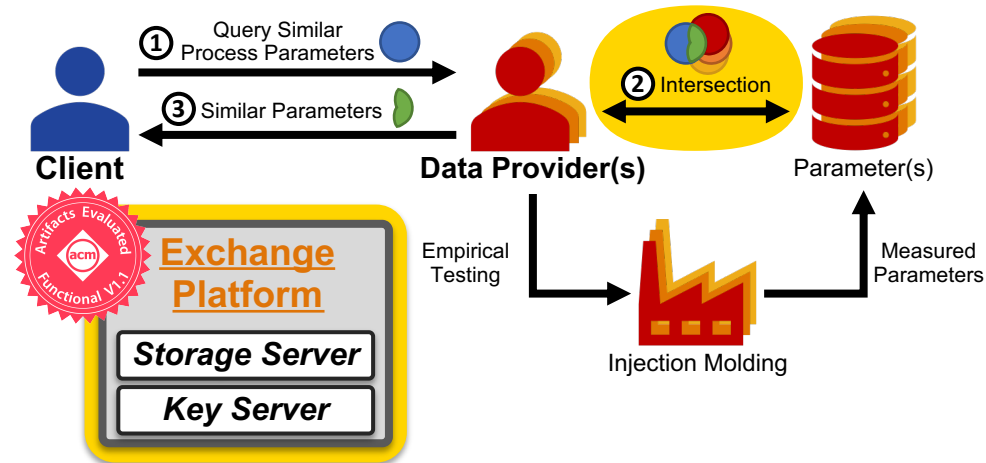


- Isolated knowledge
- Currently no privacy-preserving access
  - ▶ Concerns about data leaks, loss of control, ...

- **Real-world applicable privacy-preserving parameter exchange**

- ▶ Developed with industry needs in mind
- ▶ Scalable & universal as demonstrated with two real-world use cases

**Thursday, Session 4B:**  
Distributed Systems and Cloud Security



- **Parameter Exchange**

- 📄 [ACSAC 2020](#) (evaluated using two use cases)

- **Supply Chain Privacy**

- 📄 [BIoTCPS 2020](#) (evaluated using a fine blanking line)

- 📄 *under submission*: with a manufacturer of electric vehicles

- **Industrial Security Measurements**

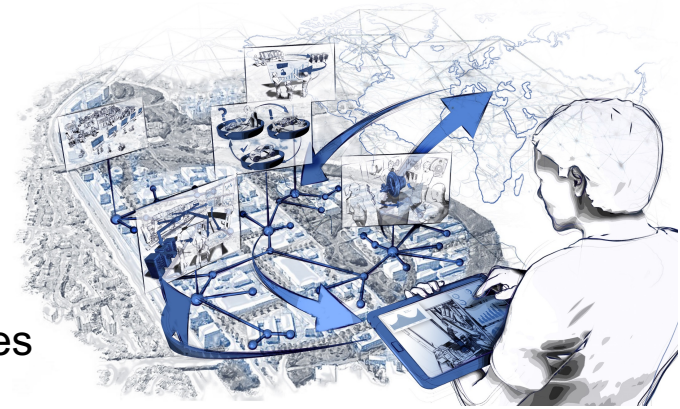
- 📄 [IMC 2020](#) (including responsible disclosure)

- **Company Benchmarking**

- 📄 [WAHC 2020](#) (with a real-world benchmark in injection molding)

- **In-Network Processing Application**

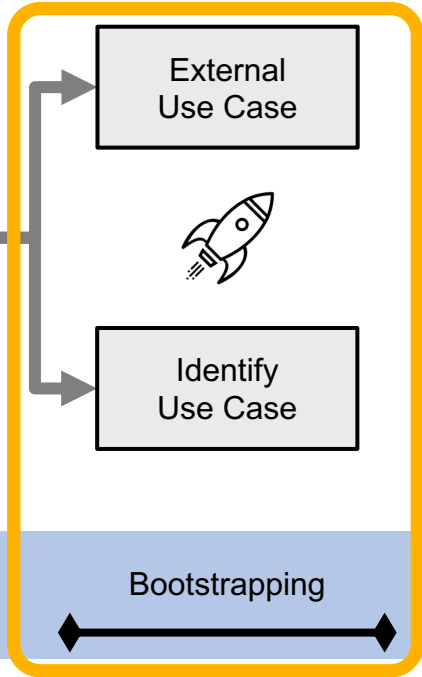
- 📄 *under submission*: improving a large-scale metrology application



## **Interdisciplinary Research Cluster**

30+ institutes (200 scientists) from various domains  
(mechanical engineering, material science, ...)

# Towards a Process Cycle of Applied Security Research



Do not hesitate to interrupt us  
with **questions** or **comments**



## A External opportunity

- ▶ Get approached by a practitioner
- **Might be a rare situation**
  - ▶ Today's security possibilities are unclear
  - ▶ Conservative companies lack visions



ACSAC

## B Identify a research gap yourself

- ▶ Challenging without domain knowledge
- **Idea identified through related work**
  - ▶ No guarantee to match industry needs



BloTCPS

## Takeaway:

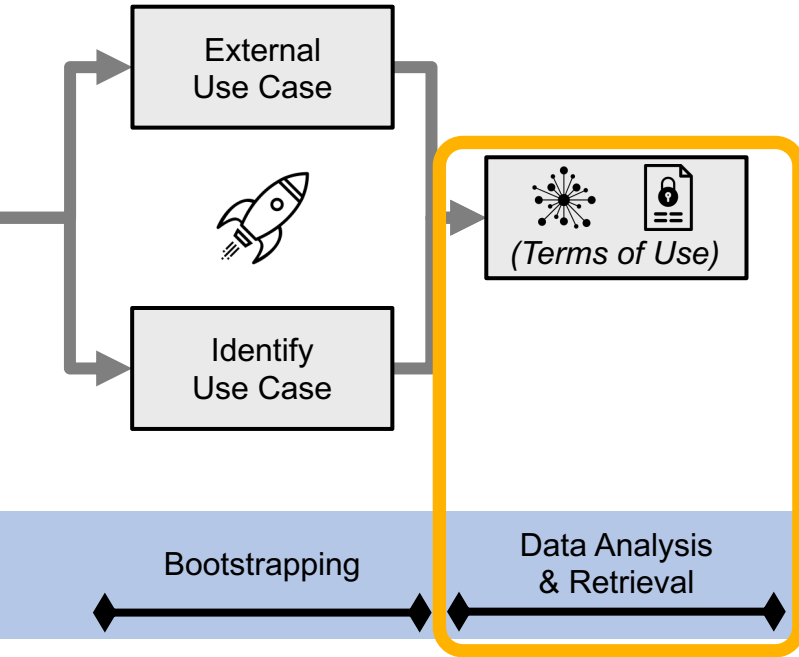
- **Identifying use cases is not trivial**
  - ▶ Requires *some* domain knowledge
  - ▶ Researcher and practitioners might not share/understand realistic *visions*
- **Do your homework!**
  - ▶ Look for suitable existing solutions
  - ▶ Identify similar use cases

We were approached by an injection molding practitioner and identified a 2<sup>nd</sup> use case (machine tools) later.



ACSAC

# Towards a Process Cycle of Applied Security Research





## • Understand what's relevant

- ▶ Practitioners might not know either
- ▶ Be prepared for *no documentation*

## • Translate (received) information

- ▶ Might be available in Excel only ☺
- ▶ The first glance might be misleading

```
# Scaled data pickled with Python 3.7.
```

```
import pickle
test = pickle.load(open('Data_w_g.pkl', 'rb'))
```

```
{'1x1_Original': {'x': [[101.0567, 173.0, 226.0, 26.0, 4.9, 18.3], [200.0567, 173.0, 226.0, 26.0, 4.9, 18.3], [101.0567, 527.0, 226.0, 26.0, 4.9, 18.3], [200.0567, 527.0, 226.0, 26.0, 4.9, 18.3], [101.0567, 173.0, 254.0, 26.0, 4.9, 18.3], [200.0567, 173.0, 254.0, 26.0, 4.9, 18.3], [200.0567, 527.0, 254.0, 26.0, 4.9, 18.3], [101.0567, 527.0, 254.0, 26.0, 4.9, 18.3], [200.0567, 173.0, 226.0, 54.0, 4.9, 18.3], [101.0567, 527.0, 226.0, 54.0, 4.9, 18.3], [200.0567, 527.0, 226.0, 54.0, 4.9, 18.3], [101.0567, 173.0, 254.0, 54.0, 4.9, 18.3], [200.0567, 173.0, 254.0, 54.0, 4.9, 18.3], [101.0567, 527.0, 254.0, 54.0, 4.9, 18.3], [200.0567, 527.0, 254.0, 54.0, 4.9, 18.3], [101.0567, 173.0, 226.0, 26.0, 14.1, 18.3], [200.0567, 173.0, 226.0, 26.0, 14.1, 18.3], [101.0567, 527.0, 226.0, 26.0, 14.1, 18.3], [200.0567, 527.0, 226.0, 26.0, 14.1, 18.3], [101.0567, 173.0, 254.0, 26.0, 14.1, 18.3], [200.0567, 173.0, 254.0, 26.0, 14.1, 18.3], [101.0567, 527.0, 254.0, 26.0, 14.1, 18.3], [200.0567, 527.0, 254.0, 26.0, 14.1, 18.3]]}}
```

	A	B	C	D
1	Name	(unique!)	1x1_Brick	1x2_Brick
2	Characteristic	(unique!)		
3	Length	[mm]	30	30
4	Width	[mm]	30	60
5	Height	[mm]	59	59
6	Volume	[mm <sup>3</sup> ]	12,496,949	21,866,305
7	Shot Volume	[mm <sup>3</sup> ]	12,496,949	21,866,305
8	Average Wall Thickness	[mm]	1,962,849,116	1,968,220,603
9	Max Wall Thickness	[mm]	2	4
10	Min Wall Thickness	[mm]	2	2
11	Flow Distance	[mm]	56,4	61,4



## Takeaway:

- Identifying & getting data is hard
  - ▶ Is it even available/accessible?
  - ▶ Are we permitted to use it?
  - ▶ What kind of processing is needed?
- Thoroughly discuss the use case data and its semantics
  - ▶ A correct understanding is key!
  - ▶ Any impact on productive systems?
- Apply the required pre-processing



- **Recap: Companies might be conservative**
  - ▶ Data is valuable (overall) and sensitive at the same time!
- **Initial meetings are usually enthusiastic**
  - ▶ However: A non-disclosure agreement might be needed

## The Bad



- **Time-consuming process**
  - ▶ Stakeholders can have different goals
- **Possibly with impact on the publication**
  - ▶ Mandatory (lengthy) approval processes
  - ▶ Might prevent to publish (negative) findings
- **Legal matters can also affect later dissemination or open-sourcing**

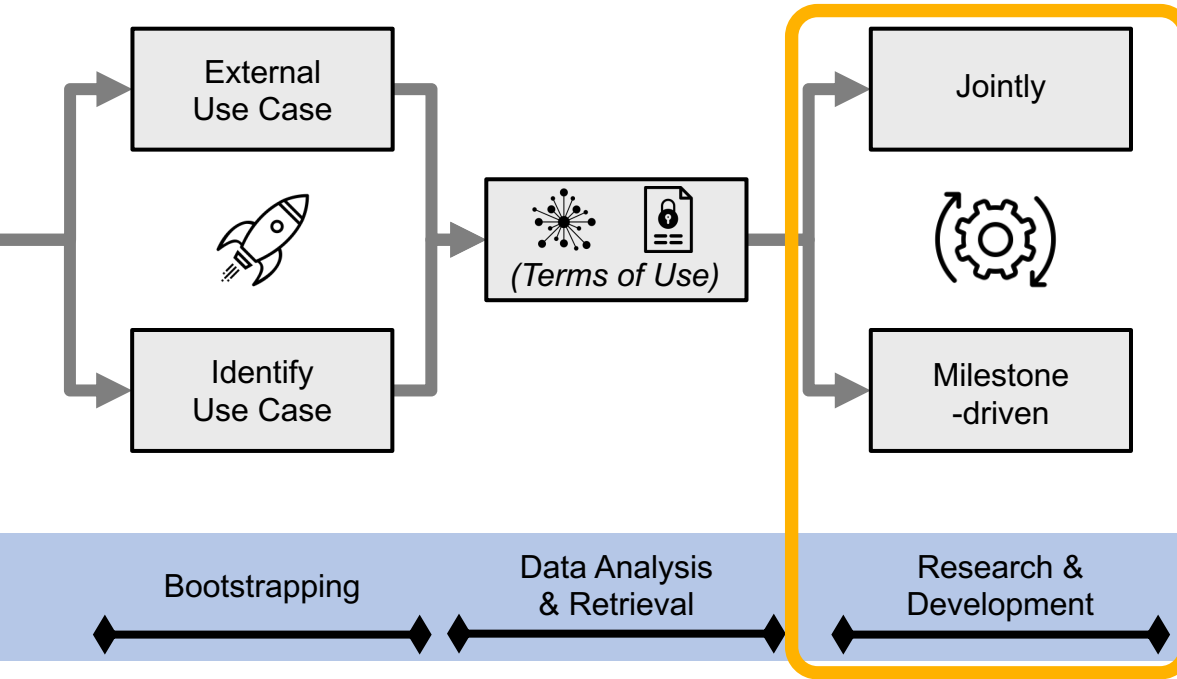


## The Good

- **You have a use case to work on 😊**
- **You get access to usually “secret” data**



# Towards a Process Cycle of Applied Security Research



#### A Joint feedback loop in place

- **Agile process extremely helpful**
  - ▶ Correct *still* existing misconceptions
  - ▶ Ability to demonstrate increments



#### B Present milestones only

- ▶ In our case a finished prototype
- ▶ Risk of solving the wrong “problem”
- **Tiresome to get evaluation data**
  - ▶ Artificial examples cannot make up for real-world use case data



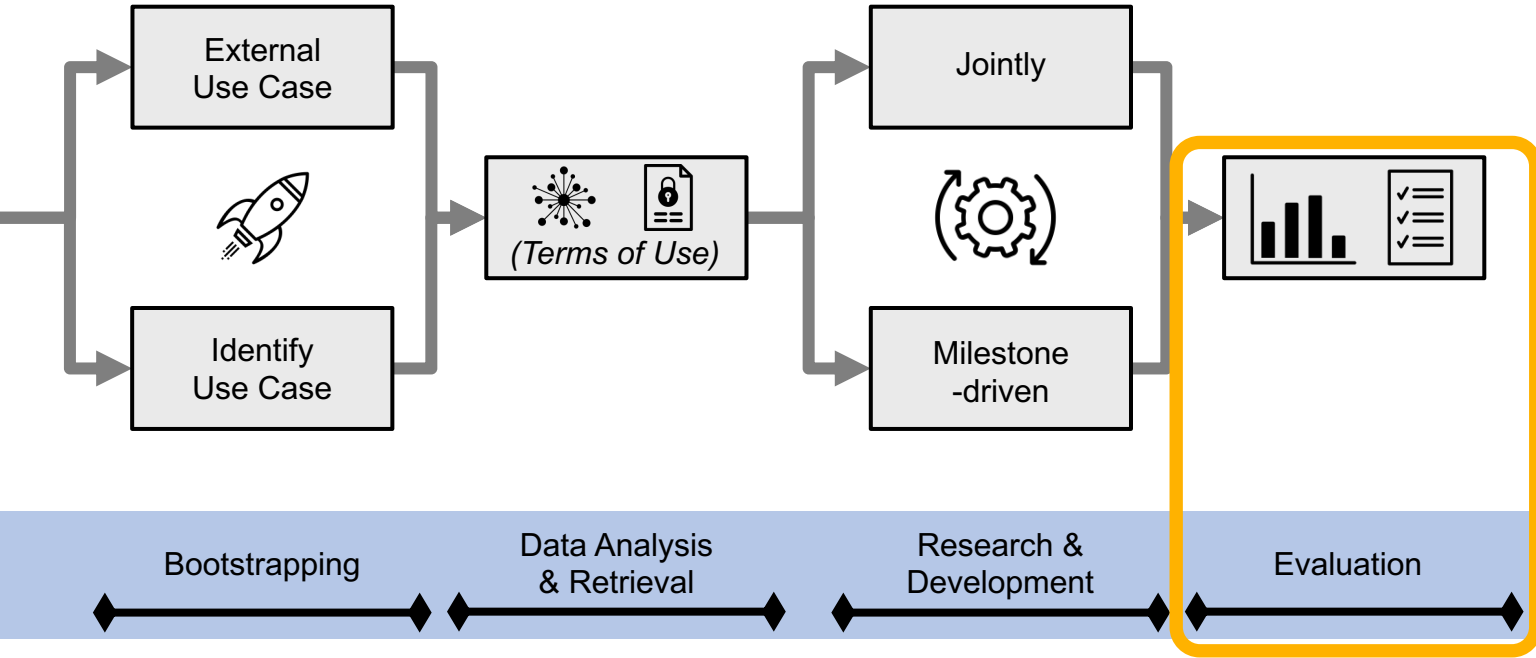
#### Takeaway:

- **A feedback loop is very beneficial**
  - ▶ Allows to fix mistakes in time
  - ▶ Practitioners feel more integrated, fewer risks of dissatisfaction
- **Scalability needs can be unclear**
  - ▶ Future developments still uncertain

A well-communicated development cycle for both sides, with the opportunity to still steer the process.



# Towards a Process Cycle of Applied Security Research



- **Can take significant time!**
  - ▶ We operated on real-world data
  - ▶ Possibly requires access to industrial machines (in production)
- **What do the results entail?**
  - ▶ Consequences for the use case
  - ▶ Are they generalizable/universal?
    - Empirical proof is hard to achieve
- **Consider safety aspects**
  - ▶ Of course, also in all other steps



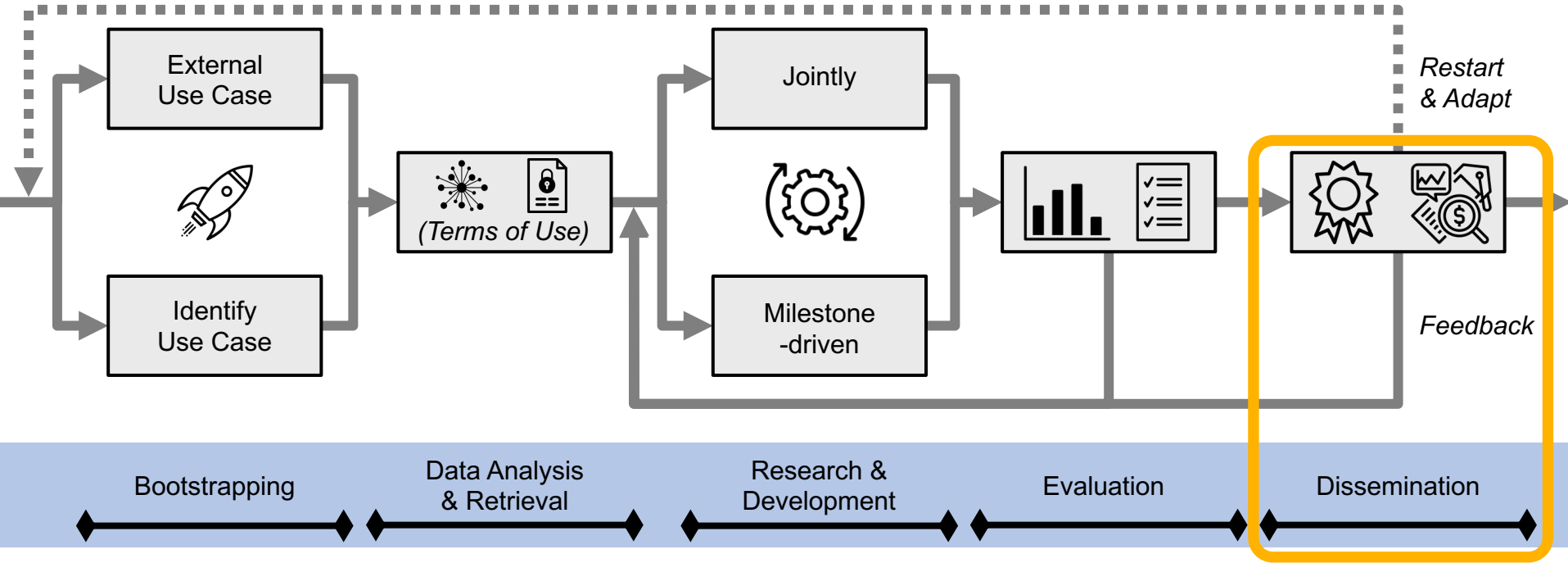
### Takeaway:

- **Check for real-world applicability**
  - ▶ Ideally using original data
  - ▶ Is the prototype really suitable?
- **Highlight and evaluate use case-independent security contribution**
  - ▶ Try to generalize as much as you can

Strong privacy is not feasible for certain real-world settings. Thus, we sacrifice some provider privacy for a 2<sup>nd</sup> universal design.



# Towards a Process Cycle of Applied Security Research





- **Research “prototype” only**
  - ▶ Open-sourced and artifacts evaluated
  - ▶ Trade-off between usability and impact for research needs consideration
    - Especially with practitioners as partners!
- **Data set-specific challenges**
  - ▶ Remove all critical/leaking aspects
  - ▶ What about transferability?
    - Other related use cases work differently!
- **Encourage more work in this area** 😊



### Takeaway:

- **Should be discussed early on**
  - ▶ Artifacts improve the submission!
- **As always, invest as little as possible but as much as needed**
- **Utilize experience to bootstrap new, more challenging use cases**



[github.com/COMSYS/parameter-exchange](https://github.com/COMSYS/parameter-exchange)

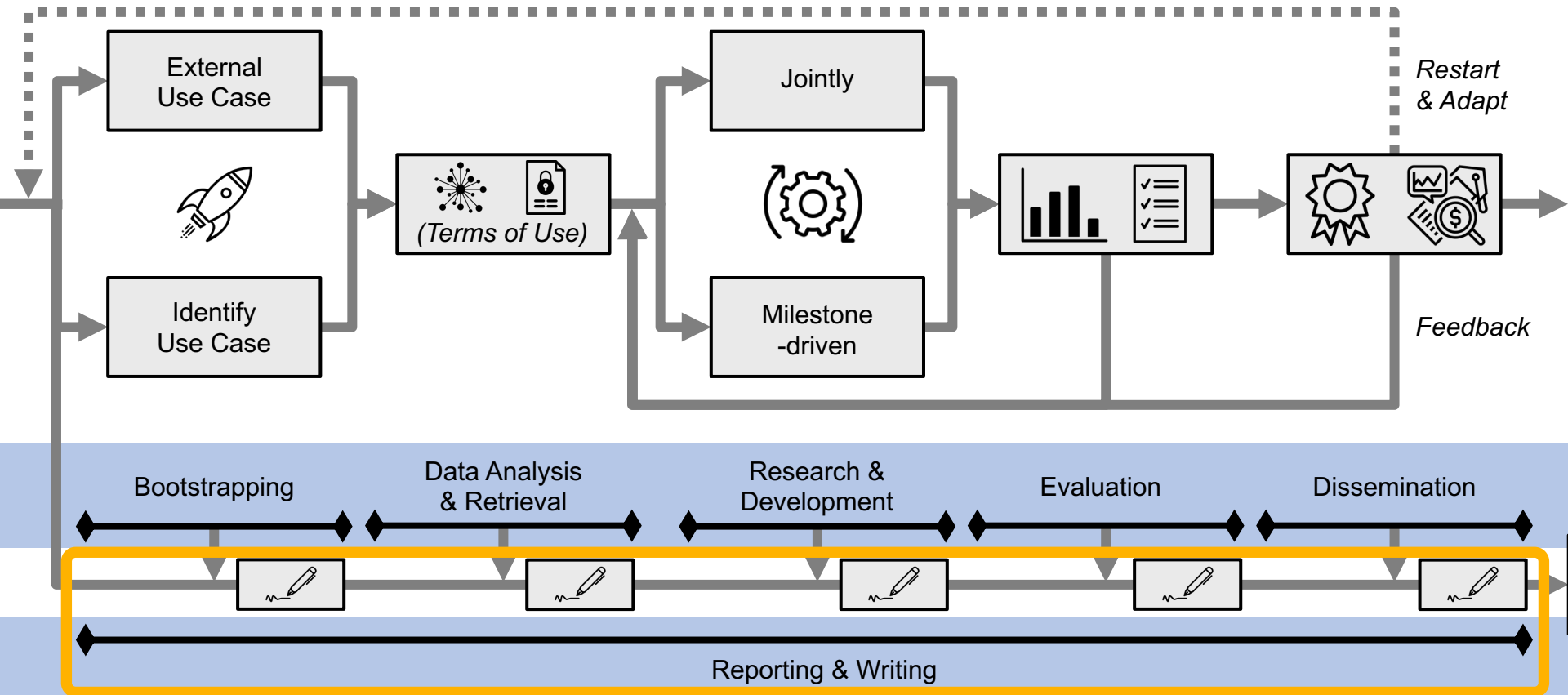
Code + Data is publicly available.



ACSAC



# Towards a Process Cycle of Applied Security Research



- **Organization is challenging**

- ▶ Different best practices in place
  - Used tools: LaTeX vs. Word, versioning, ...
- ▶ (Re-)Approval can take significant time

- **Where to submit?**

- ▶ Security contribution should be the driver, but partly seen as very applied research
- ▶ Identify a suitable community and venue
- ▶ Reviewers might not understand the practical impact in the application domain



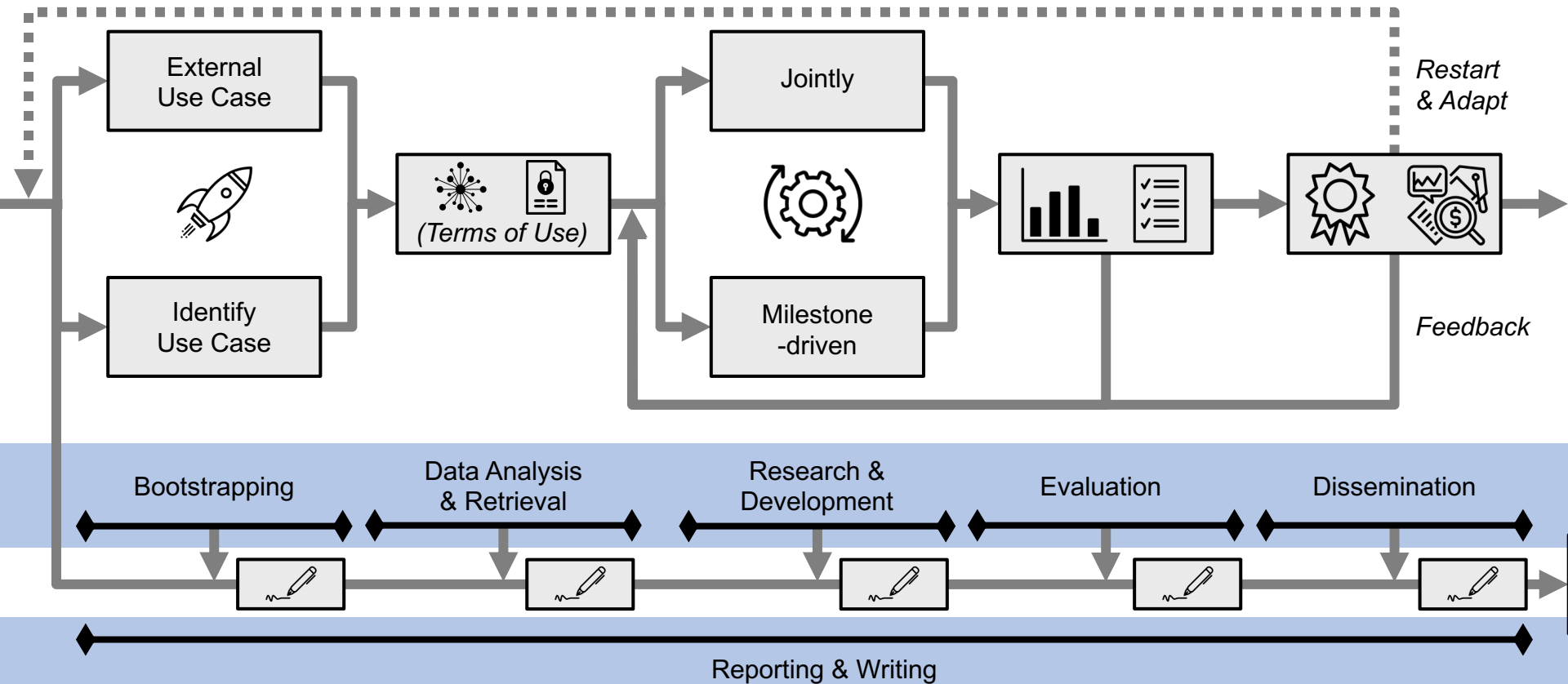
### Takeaway:

- **Challenging to work in parallel**
  - ▶ Due to approval and feedback loops
- **No last minute changes!**
  - ▶ Prepare yourself (early on)
  - ▶ Communicate clear expectations
- **Consider to submit two papers**
  - ▶ Focus on individual contributions each

Final publication with 9 authors from 3 departments: Differing publication cultures and expectations.



# The Complete Process Cycle of Applied Security Research



## Questions so far?

- **Communication is key**
  - ▶ Implicit assumptions (e.g., about existing domain knowledge, realizability, and requirements concerning use case data) from both sides
  - ▶ Might be a sign for “cutting-edge” research
- **Do not take anything for granted**
  - ▶ Wording / notation / terminology might differ between the domains  
Unfortunately, it is quite challenging to bridge them and it takes time
- **Re-using datasets and existing artifacts can be challenging**
  - ▶ Mostly little documentation available
  - ▶ Specific details are missing
  - ▶ Overall, only few resources exist



**Progress in *secure* industrial collaboration is achievable by carefully bridging the domains**

- **Do you consider security research for industrial collaborations worthwhile?**
- **Are you interested in collaborating on real-world use cases, or are the interdisciplinary challenges and domain differences not worth the effort?**
- **Are we missing any fundamental (yet trivial?) steps in our process cycle?**
- **Did you ever experience the challenge to identify a fitting community or to find a venue for your (interdisciplinary) work?**
- **What is your take on non-disclosure agreements in research?**

- **Next steps**

- ▶ Getting the currently unpublished papers published 😊
- ▶ Looking for additional feedback from YOU



Are *YOU*  
willing to  
contribute?

- **Post-workshop paper**

- ▶ A more detailed description of our “findings” and the individual steps
  - Underlined with multiple real-world examples / collaborations
- ▶ Integrating input from one or multiple collaborators (considering their applied views)
- ▶ Potentially integrate the needs of RDM (research data management) concerning the intersection of security research and applied industry use cases

**Thank you for your attention!**